IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

RIDING FILMS INC. Plaintiff, v. DOES 1-65 Defendants	)))))Case No: 13-00288))))

DECLARATION OF DARREN M. GRIFFIN PURSUANT TO 28 U.S.C. § 1746 IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

1. My name is Darren M. Griffin. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate. I am I am a software consultant with nine years of experience working in the field. I have a degree in computer science.

2. I have been retained as a software consultant by Crystal Bay Cooperation ("Crystal Bay"), a corporation incorporated and currently in good standing in South Dakota and organized and existing under the laws of the United States, in its technical department. Crystal Bay is in the business of providing forensic investigation services to copyright owners. Crystal Bay is a provider of online anti-piracy services for the Motion Picture industry to monitor infringing activity. Crystal Bay has been retained to investigate infringements of copyrights owned by the Plaintiff in this matter.

3. The Internet is a vast collection of interconnected computers and computer networks that

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted works, including music and film.

4. Once a Motion Picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

5. To copy and distribute copyrighted Motion Pictures over the Internet, many individuals use online media distribution systems or so-called Peer-to-Peer ("P2P") networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including Motion Pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

6. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

7. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to an unlimited amount of other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

8. Further, a person who uses a P2P network is free to use any alias (or

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

"network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

9. Additionally, the P2P methodologies for which Crystal Bay monitored for Plaintiff's Motion Picture, known as "BitTorrent," make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download the file. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional peer-to-peer network (e.g. Napster, KaaZa, and Limewire), each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which is pieced together by P2P software to comprise the whole.

10. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network – or even a portion of a copy – can also be a source of download for that infringing file, potentially both copying and distributing the infringing work simultaneously. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

11. On behalf of Plaintiff, Crystal Bay engaged in a specific process utilizing its specially

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

designed software technology to identify direct infringers of Plaintiff's copyrights on P2P networks. All of the infringers named as Doe Defendants were identified in the following way: Crystal Bay software is connected to files of infringing versions of the Motion Picture. All infringers connected to those files are investigated through downloading a part of the file placed on their computer. This evidence is then saved by Crystal Bay.

12. Once Crystal Bay's searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay obtains the IP address of a user offering the file for download.

13. The forensic software used by Crystal Bay routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works. Among other things, for each file downloaded, Crystal Bay downloads or records: (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to or contained within the digital file and helps identify the content of the file. Crystal Bay then creates evidence logs for each user and stores this information in a database.

14. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon or AT&T, an Internet service provider such as America Online, a cable Internet service provider such as Comcast or

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

Time Warner, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

15. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

16. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IANA") or a regional internet registry such as the American Registry for Internet Numbers ("ARIN"). ISPs keep track of the IP addresses assigned to their subscribers at any given moment and retain such "user logs" for a very limited amount of time, sometimes as little as weeks or even days, before erasing the data they contain. These user logs provide the most accurate – and often the only – means to connect an infringer's identity to its infringing activity.

17. Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable from the packets of publicly available data being exchanged. The exact manner in which Crystal Bay determines a user's IP address varies by P2P network. An infringer's IP address is significant because it is a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the Motion Picture itself, Crystal Bay downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. Crystal Bay determined that the Doe Defendants here were using ISPs listed in Exhibit A filed with the Complaint to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted Motion Picture.

21. Here, the IP addresses Crystal Bay identified for Plaintiff enable Crystal Bay to determine which ISP was used by each infringer to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate some of their IP addresses to other unrelated, intermediary ISPs. Since these ISPs consequently have no direct relationship – customer, contractual, or otherwise – with the end-user, they are unable to identify the Doe Defendants through reference to their user logs, but they can identify the intermediary ISP to which that IP address has been allocated. Therefore, the intermediary ISPs' own user logs should permit identification of the Doe Defendants.

22. Once Crystal Bay identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity. Once

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

provided with the IP address, plus the date and time of the infringing activity, the Doe Defendants' ISPs quickly and easily can use their respective subscriber logs to identify the name.

23. Crystal Bay determined that the Doe Defendants in this matter were using ISPs listed in Exhibit A filed with the Complaint to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted Motion Picture. Crystal Bay then downloaded the Motion Picture file, or a substantial part of it, and other identifying information described above and created evidence logs for each Doe Defendant. After Crystal Bay identified the Doe Defendants and downloaded the Motion Picture files they were distributing, Crystal Bay opened the downloaded files, watched them and confirmed that they contain a substantial portion of the Motion Picture.

24. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which Motion Picture is copied in the downloaded file, but confirms the infringement through a visual comparison between the downloaded file and the Motion Picture themselves. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay watches a DVD copy of the Motion Picture provided by Plaintiff and compares it to the downloaded files to insure that such files contain a substantial portion of the Motion Picture.

25. Plaintiff retained Crystal Bay to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted Motion Picture as identified in Episode 50 (the "Motion Picture"). Crystal Bay tasked me with analyzing, reviewing and attesting to the results of the investigation. During the performance of my duties as detailed below, I used forensic software provided by Crystal Bay to scan peer-to-peer networks for the presence of

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

infringing transactions. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Motion Picture. Through each of the transactions, the computers using the IP addresses identified in Exhibit A filed with the complaint transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit A filed with the complaint. The IP addresses, hash values, dates and times contained in Exhibit 1 correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit A filed with the complaint were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the Motion Picture.

26. Moreover, in most if not all of the cases, the users were sharing the exact same copy of the Motion Picture. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Motion Picture, I confirmed that these users reproduced the very same copy of the Motion Picture.

27. The Crystal Bay software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit 1 and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital Motion Picture file. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit A filed with the complaint were located in Washington within this district. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975

public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs. As set forth in Exhibit A filed with the complaint, I have confirmed not only that the users distributed the files in Washington, but also the specific location where the distribution took place.

28. Plaintiff has engaged Crystal Bay to continue monitoring efforts. As such, Crystal Bay's monitoring efforts for Plaintiff's copyrighted works, including but not limited to the Motion Picture, are continuing.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 15 day of February, 2013.

By: ______________________
Darren M. Griffin

Frontier Law Group, PLLC
1001 Fourth Avenue, Suite 3200
Seattle, WA 98154
Ph: 206-682-7975